Paper Number 2004-01-01

AN OPEN SYSTEMS APPROACH TO SAFETY MANAGEMENT

Gavan Lintern
Advanced Information Engineering Services, Inc
General Dynamics
Dayton, Ohio

All major system accidents have, as one contributing factor, a failure of operational personnel to adhere to certain critical procedures. The typical response is to develop more detailed constraints in an attempt to prevent reoccurrence of that sort of accident. This approach exemplifies the worst of rule-based safety management. It is retroactive and fails to recognize the strength of lessons learned by operational personnel in practice. Safety management must embrace a proactive strategy that takes account of the strength of on-the-job adaptation. Nevertheless, rule-based safety management based on principles of rational design cannot be dismissed entirely. It does produce a globally coherent rule set that can be degraded by local adaptations. In this paper I discuss an open-systems approach to safety management, one that reveals effects of local operational adaptations on global constraints to all participants within the system and also promotes global validation of local adaptations before they are permitted to become entrenched. By this means, it will be possible to build a robust and efficient system through an evolutionary process while at the same time, avoiding reliance on brittle and mutually incompatible rule sets that actually compromise safety.

Safety Management

> "…the problem of rules created by those who do not have to live the life"
>
> John Irving, discussing a dominant theme of his novel, The Cider House Rules

Reviews of major system accidents almost always implicate failures of operational and management staff to adhere to critical procedures or best practice allied with their failure to appreciate the significance of potential system interdependencies. Typically, there is a drift in best management and operational practice as the rigor that characterizes the early deployment of a system is eroded by the burgeoning demands of ongoing operations. However, current approaches to safety management generally fail to take account of two pervasive properties of complex socio-technical systems, firstly that the human participants are constantly changing the system, and secondly that this process of change, emerging from experience, has enormous (and generally untapped) potential to **enhance** safety.

The changing nature of socio-technical systems

Human collaborative systems are inevitably open to the generation of new properties. The ***openness*** of a complex socio-technical system is a source of latent pathogens (Reason, 1997) that can amplify the effects of seemingly normal events to the point that they reverberate through the system in ways never imagined by designers or operators. The fundamental assumption of the argument I present here is that we have neglected this openness and that we continue to pay a price for that neglect.

Most approaches to safety management attempt to lock the system down so that it does not generate new properties. This is done by the imposition of detailed rule sets derived from rational analysis, a strategy that can work well in the case of orderly, non-critical systems (even if they are open) and can appear to work for a considerable time in open, safety-critical systems. However, open systems are infinitely generative. Thus, we cannot construct a rule set that will incorporate all possibilities. Worse, the attempt to be comprehensive can produce such a large rule set that its very size confounds those who must work with it.

The potency of operational experience

Once deployed, rule sets become established as ***the formal way*** of doing things. There is generally no recursive mechanism to feed ***lessons learned in practice*** back into the redesign or retuning of the system. Procedures developed from a rational analysis of requirements rather than from within practice itself are often clumsy, fragile and incomplete.

A contrast to rational analysis can be found within aviation where aircrews develop procedures as they work out how to accomplish specific tasks. Procedures developed in this manner constitute abbreviated descriptions of expert performances. They provide a detailed and well-crafted plan of action that is robust and efficient (Lintern & Naikar, 2001). Aviation has led the way in the development of robust procedures from distillation of actual practice. Nevertheless, local adaptation via procedures developed in practice is contrary to the philosophy of rational design and often generates informal mechanisms that directly oppose the expressed goals and values of safety management (McDonald, Corrigan & Ward, 2002).

Procedural Drift

Success in dealing with the issues of openness and the fragility of rational procedures will constitute a much-desired paradigm shift in safety management. Much as a martial arts expert uses the thrust of an opponent to advantage, ***lessons learned in practice*** could be fed back into redesign of the system, thereby improving safety by enhancing robustness of procedures while, at the same time, accommodating to the openness of the system.

The essential problem I confront here is that design of any new system is generally driven by rational considerations of designers who either are not practitioners or who are not currently involved in practice (Lintern, 1995). The rational system, once deployed, will be reshaped in practice by local pressures. In a distributed system, local practice will drift to become disconnected from global constraints. This is possibly the major threat to safety in today's complex socio-technical systems (Rasmussen, Pejtersen & Goodstein, 1994; Reason, 1997).

All past and contemporary approaches to safety seek to eliminate the drift generated by local pressures through use of tight control in the form of rules and procedures. The approach I offer here seeks to exploit that drift (to permit it to function as a local means of developing robust and efficient procedures) but to guide it by maintaining explicit connection to global constraints. Thus, the strengths of operational practice would be coordinated with the strengths of rational design to enhance system design, operational practice, and system redesign.

A case study

A stimulus for this approach, one that illustrates the need and the challenges, is an analysis by Snook (2000) of the destruction of two US Army Black Hawk helicopters over Northern Iraq by two USAF F-15s on 14th April 1994 during **Operation Provide Comfort**. All on board the Black Hawk helicopters (which included a number of UN peacekeepers) perished in this accident. The accident occurred despite AWACS coverage and despite a host of carefully designed procedures that should have prevented it.

The F-15s involved in this accident were assigned the task of sanitizing the operational area, i.e. of ensuring there were no enemy aircraft and that it was safe for other allied flights. Although the F-15 flight was to be the first into the area that day, the two Black Hawks were already there. The F-15 pilots asked at three different times whether there were any adjustments to the Air Tasking Order (which did not identify the Black Hawk operation) and were advised there were not. One of those requests went to the AWACS team who knew of the Black Hawk operation. The AWACS team followed the engagement without raising the possibility that these two helicopters, read by the F-15 pilots as hostile, were in fact US aircraft. All this unfolded against a backdrop of no enemy incursions into this space in a considerable time.

Procedural drift in complex systems

Analyses of this accident (Snook, 2000; Leveson, Allen & Storey, 2002) reveal the challenges facing the design and operation of complex, socio-technical systems. Although the original design of procedures (as embedded in the Operations Plans for Operation Provide Comfort) appeared to be sound, local pressures of operational practice induced a drift to locally efficient but globally inconsistent procedures. Snook (2000) argues that this process is inevitable and posits an engine that cycles through four states:

1. Planners assume a ***tightly coupled*** system in which interdependent processes affect each other directly and immediately. Given that assumption, planners over-design the system as a conservative approach to reducing the possibility of accidents from interactions of tightly coupled processes. Finally, planners assume that operational personnel will follow procedures as specified.

Operational personnel initially assume that all rules are justified and that failure to follow the rules will have severe consequences (beyond those of disciplinary action). However, the system is predominantly ***loosely coupled*** and the rules not well tuned to operational practice. Operational personnel come to believe through their own experience that strict adherence to the rules is unnecessary. They subsequently implement local adaptations, which then become the locally accepted ways of doing things. Snook refers to this process as ***Practical Drift***. Following Johnston (2003), ***Procedural Drift*** is preferred in this paper as a term better suited to aviation.

2. While the system is **predominantly** loosely coupled, it is not entirely so. Occasional circumstances bring normal processes into an unusual (but not extraordinary) confluence of tightly coupled systems. Because the global rationality of the **system-as-designed** has been degraded, the **local adaptations** permit the now tightly coupled processes to interact in unfortunate ways, often resulting in an incident or accident.

The management response to any ensuing accident is to re-establish global rationality by writing and then more strictly enforcing an enhanced rule set. This effort reestablishes global control but increases the force that generates Procedural Drift.

This engine might be seen as a behavioral pump with four cylinders (Figure 1) in which the motive force is drawn from the ecology of the system, where rational logic is overcome by what we might call an ***eco-logic***. From this perspective, Procedural Drift is pervasive in complex socio-technical systems that are predominantly loosely coupled. Rasmussen, et al. (1994) view this as an inevitable migration towards the boundaries of safe operation where serious consequences can result if occasional but normal circumstances bring processes into an unusual confluence of tightly coupled systems.

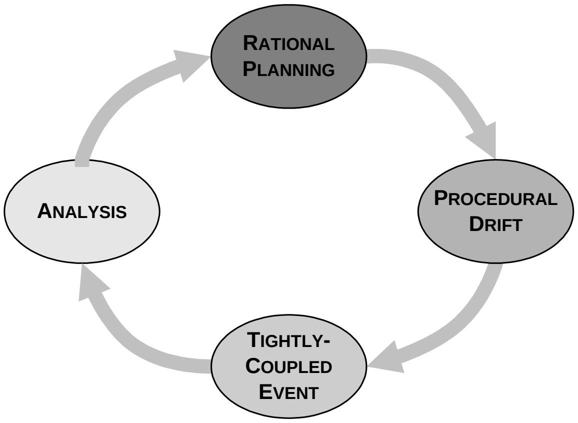

Figure 1: Local practice becomes disconnected from global constraints through a cycle of Rational Planning → Procedural Drift → Tightly Coupled Event → Analysis → Rational Planning → ……

Procedural Drift in Operation Provide Comfort

> "Well Homer, you're the only one who's read those rules and so you're the only one feeling guilty."
>
> Arthur Rose, Crew Boss (played by Delroy Lindo) in the film version of The Cider House Rules

Procedural Drift was widespread in Operation Provide Comfort, seemingly influencing local operations in all corners of the system. For example, Army and Air Force operations were poorly integrated and the natural consequence was a drift to localized operational procedures that were not mutually compatible. Army pilots were unaware of the correct procedure in relation to Identify Friend or Foe (IFF) and failed to fully understand the implications of the sanitizing role that the USAF had in ensuring the operational area was clear of enemy aircraft. The failure to coordinate IFF codes was identified as one of the many significant events in the destruction of the Black Hawks.

Systemic Issues

> "... operators would not always follow the written procedures … because the desired goal would not be achieved … (they were) criticized for "lack of procedural compliance. The operators decided they would do exactly what the procedure said … became stuck in an infinite loop … criticized… yet again …for 'malicious procedural compliance.'"
>
> Vicente (1999), Cognitive Work Analysis, p xv

The processes used to develop procedures for Operation Provide Comfort are typical of design approaches to complex, large-scale socio-technical systems. Johnston (2003) describes a number of aviation issues that illustrate the pervasive problems:

- Systems are over-designed with an unnecessarily complex overlay of rules and procedures.
- The extensive documentation that publishes rules and procedures seems comprehensive but is not.
- The polite fiction is maintained that operational personnel are fully conversant with this documentation whereas casual analysis suggests that no one could possibly be fully conversant with such an extensive (and fluid) set of documentation.
- It is assumed that rational planning can produce robust and effective procedures. However, procedures developed by rational planning are often clumsy and fragile.
- Although it is assumed that complex socio-technical systems such as Operation Provide Comfort are static, many dynamic forces are at work to force continual change.
- The inevitability of local adaptation is not acknowledged and so there is no global oversight to ensure that local adaptations remain consistent with global constraints.
- Local adaptations emerge from lessons learned in practice, which is widely recognized as a powerful force for tuning effective behavior, but no mechanism is established for feeding the lessons of operational experience back into a global system update.

It is ironic that a design philosophy oriented towards ensuring safety produces so many system features that actually compromise safety.

Today's Typical Response

Safety management appears to be locked in a wrong-headed approach of retrospective analysis followed by development of more intricate control. The typical adjustment following an incident such as the destruction of the Black Hawk helicopters in Northern Iraq is to develop more rules to eliminate the possibility of a repeat incident of that type. This approach ignores Perrow (1984) who argues that larger, more complex rule sets can actually increase the risk of serious incident. Figure 1 supports Perrow's claims by depicting a process in which rational planning feeds the motive force of procedural drift. However, even after an extensive and insightful analysis, Snook (2000) is at a loss about how to rectify the situation.

Safety Management: An Open Systems Approach

Scientific approaches to safety research emphasize a retroactive, control-based philosophy. Leveson, et al. (2002), who reviewed the loss of the Black Hawk helicopters over Northern Iraq, have developed a model in which accidents are viewed as resulting from a lack of constraints imposed on the system design and operations, and are attributed to incomplete specification at one or more levels of the organizational hierarchy. This approach fails to recognize that major accidents result not from incomplete specification within the organizational hierarchy but because local decisions in the absence of global oversight subvert its integrity.

Elsewhere I have argued for a proactive, open systems approach to safety management based on a structured knowledge visualization and a global audit process that would identify local adaptations and confirm that they remain consistent with global constraints (Lintern, 2003, also see Figure 2). The knowledge visualization would need to be comprehensive and integrated and would have to reveal global and local constraints and also the interplay between them.

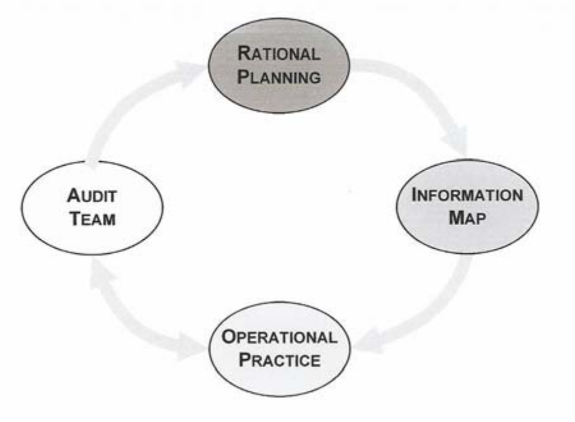

Figure 2: A proactive, open systems approach to safety management relies on a two-way process between operational practice and the audit team.

A current issue: Space shuttle management

Space shuttle management has attracted significant criticism following the losses of Challenger and Columbia. This criticism is, however, a new version of the historical (and widely discredited) impetus to blame the operator. It offers minimal insight into the challenges faced by managers within a complex, socio-technical system. One disconcerting challenge faced by managers as they confront safety related issues is to separate the signal from the noise, a challenge for which they are offered very little effective support.

After each of the two space shuttle accidents, management procedures were judged to have drifted from best practice as rationally defined, an observation that mirrors the blame directed at operators in cases where they have been judged at fault for an accident. Drift in management procedures is a type of operational drift that occurs in all complex socio-technical systems and at all levels of the organizational hierarchy.

The danger in the current climate is that drift will be viewed as the problem and that a new style of decision process will be imposed. In all likelihood, it will be a rational and globally coherent process but one that is brittle and inefficient.

Cognitive Tools for Organizational Decisions

> … we are now responsible for so many decisions requiring so much homework that many of us feel helpless and paralyzed. The risks of inaction or unwise action are rising…
>
> Daniel Kadlec, Time Magazine, January 28, 2002, pages 24-28

The drift in management decision procedures is forced on the system by the cognitive overload placed on decision makers at all levels. This cognitive overload arises partially out of the competing demands that assail all in a high intensity work place but is exacerbated by fragmented, poorly organized arguments set within a context of incomplete, inaccurate, and fragmented information. The result is that a considerable number of organizational decisions are based primarily on unsupported conviction or persuasion rather than on the imperative of concise and pertinent information.

A structured knowledge visualization

The functioning of complex socio-technical systems relies on such diverse and independent areas of expertise that some form of collaborative tool is essential to facilitate robust and coherent assessment of the potential impact of decisions and actions on global system behavior. I propose that it must be a cognitive tool based on a knowledge visualization that is structured to support coherent assessment of the diverse functionality of the total system and recognition of dependencies and interdependencies between functional areas.

As I have argued in Lintern (2003), a knowledge visualization might be based on an Abstraction-Decomposition map, which is a knowledge representation tool developed by Jens Rasmussen (Rasmussen, et al., 1994; Vicente, 1999). The AcciMap (Svedung, & Rasmussen, 2002) also offers a possible basis for a suitable visualization. Whatever the underlying structure of the visualization, it needs to result in a cognitive tool that supports decisions within a complex, interdependent information space without promoting cognitive overload. In particular, it should help mangers, auditors and operators understand the relationship of their adaptive activities to global constraints and to local requirements of other interdependent functions.

Conclusion

All major system accidents have, as one contributing factor, a failure of operational personnel to adhere to certain critical procedures. The typical response is to develop more detailed constraints in an attempt to prevent reoccurrence of that sort of accident. This approach exemplifies the worst of rule-based safety management. It is retroactive and fails to identify the pervasive fragilities within the system structures. It also fails to recognize the strength of lessons learned by operational personnel in practice and the important contribution they cam make to building a robust system.

Safety management must embrace a proactive strategy that takes account of the strength of on-the-job adaptation. In this paper I discuss an open-systems approach to safety management, one that reveals effects of local operational adaptations on global constraints to all participants within the system and also promotes global validation of local adaptations before they are permitted to become entrenched. By this means, it will be possible to build a robust and efficient system through an evolutionary process while at the same time, avoiding promulgation of brittle and mutually incompatible rule sets that actually compromise safety.

Acknowledgement

I developed the conceptual basis for this paper while at Aptima, Inc.

Author Contact

5200 Springfield Pike, Suite 200
Dayton, Ohio 45431-1289
Gavan.Lintern@gd-ais.com

References

Johnston, N. (2003). The Paradox of Rules: Procedural Drift in Commercial Aviation. In R. Jensen, (Ed), *Proceedings of the Twelfth International Symposium on Aviation Psychology,* April 14-17, 2003*, Dayton, Ohio* [CD-ROM].

Leveson, N.G.; Allen, P. & Storey, M-A (2002). The Analysis of a Friendly Fire Accident using a Systems Model of Accidents. *International Conference of the System Safety Society*, Denver.

Lintern, G (2003). Tyranny in Rules, Autonomy in Maps: Closing the Safety Management Loop. In R. Jensen, (Ed), *Proceedings of the Twelfth International Symposium on Aviation Psychology (pp 719-724),* April 14-17, 2003, Dayton, Ohio [CD-ROM]

Lintern, G. (1995). Flight instruction: The challenge from situated cognition. *The International Journal of Aviation Psychology, 5*, 327-350.

Lintern, G. & Naikar, N. (2001). *Analysis of Crew Coordination in the F 111 Mission* (DSTO-CR-0184). Melbourne, Victoria, Australia: Aeronautical & Maritime Research Laboratories, Defence Science & Technology Organisation.

McDonald, N., Corrigan, S. & Ward, M. (2002). Cultural and Organizational factors in system safety: Good people in bad systems. *Proceedings of the 2002 International Conference on Human-Computer Interaction in Aeronautics (HCI-Aero 2002)* p 205-209. Menlo Park, CA: American Association for Artificial Intelligence Press.

Perrow, C. (1984). *Normal accidents: Living with high-risk technologies*. New York: Basic Books.

Rasmussen, J., Petjersen, A. M., & Goodstein, L. P. (1994). *Cognitive systems engineering*. New York: John Wiley.

Reason, J. (1997). *Managing the Risks of Organisational Accidents*. Aldershot, UK: Ashgate Aviation.

Snook, S.A. (2000). *Friendly Fire*. Princeton University Press.

Svedung, I., & Rasmussen, J. (2002). Graphic representation of accident scenarios: Mapping system structure and the causation of accidents. Safety Science, 40, 397-417.

Vicente, K. J. (1999). Cognitive Work Analysis: Towards safe, productive, and healthy computer-based work. Mahwah, NJ: Lawrence Erlbaum & Associates.